

## CLAIMS

## WHAT IS CLAIMED IS:

- 5 1. A system for malicious code detection, comprising:  
a plurality of scanning computer systems configured for scanning content for  
malicious code and generating an alarm when the file contains malicious code;  
and  
a front-end processor, coupled to the scanning computer systems, configured for  
receiving a flow of content from an external network and distributing copies of  
the flow to each of the scanning computer systems in parallel for scanning; and  
10 a detection management system, coupled to the scanning computer systems,  
configured for employing a countermeasure on the flow if at least one of the  
scanning computer systems generates the alarm.
- 15 2. The system according to claim 1, further comprising a database containing rules  
configured for creating a signature of a piece of malicious code detected by at least one of  
the scanning computer systems.
3. The system according to claim 2, further comprising a remote site detection  
system configured for detecting malicious code in incoming network traffic based on  
signatures of malicious code stored thereat.
- 20 4. The system according to claim 3, wherein the detection manager is further  
configured for causing the signatures stored at the remote site detection system to be  
updated to include the signature of the piece of malicious code detected by said at least  
one of the scanning computer systems.

5. The system according to claim 1, wherein each of the scanning computer system is configured to execute respective anti-virus scanning software having different, corresponding coverage of malicious code.

6. The system according to claim 1, wherein the flow includes at least one of a  
5 hypertext markup file and a transferred file.

7. The system according to claim 1, wherein the countermeasure includes at least one of blocking the flow, quarantining the flow, and informing the recipient of the flow of the malicious code.

8. A system for malicious code detection, comprising:  
10 a remote site detection system configured for detecting malicious code in incoming network traffic based on signatures of malicious code stored thereat;  
a plurality of scanning computer systems configured to execute respective anti-virus scanning software having different, corresponding coverage of malicious code for  
15 scanning content for malicious code and generating an alarm when the content contains malicious code; and  
a front-end processor, coupled to the scanning computer systems, configured for receiving a flow of content from an external network and distributing copies of the flow to each of the scanning computer systems in parallel for scanning, said  
20 flow including at least one of a hypertext markup file and a transferred file; and

a detection management system, coupled to the scanning computer systems, configured for:

creating a signature of a piece of malicious code detected by at least one of the scanning computer systems detected in the flow when at least one of the scanning computer generates an alarm on the piece of malicious code;

employing a countermeasure on the flow if at least one of the scanning computers generates an alarm on the piece of malicious code, said countermeasure including at least one of blocking the flow, quarantining the flow, and informing the recipient of the flow of the malicious code; and

causing the signatures stored at the remote site detection system to be updated to include the signature of the piece of malicious code detected by said at least one of the scanning computer systems.

9. A method for malicious code detection in a system including a plurality of scanning computer systems, comprising:

receiving a flow of content from an external network;

distributing copies of the flow to each of the scanning computer systems in parallel;

scanning the flow for malicious code and generating an alarm when the content contains malicious code at each of the scanning computer systems; and

employing a countermeasure on the flow if at least one of the scanning computer systems generates the alarm.

10. The method according to claim 9, further comprising creating a signature of a piece of malicious code detected by at least one of the scanning computer systems.

11. The method according to claim 10, further comprising detecting malicious code in incoming network traffic at a remote site detection system based on signatures of malicious code stored thereat.

12. The method according to claim 11, further comprising updating the signatures  
5 stored at the remote site detection system to include the signature of the piece of malicious code detected by said at least one of the scanning computer systems.

13. The method according to claim 9, wherein said scanning at each of the scanning computer systems includes executing respective anti-virus scanning software having different, corresponding coverage of malicious code.

10 14. The method according to claim 9, wherein the flow includes at least one of a hypertext markup file and a transferred file.

15 15. The method according to claim 9, wherein said employing the countermeasure includes at least one of blocking the flow, quarantining the flow, and informing the recipient of the flow of the malicious code.

16. A method for malicious code detection in a system including a remote site detection system and a plurality of scanning computer systems, comprising:

receiving a flow of content from an external network, said flow including at least one  
of a hypertext markup file and a transferred file;

20 distributing copies of the flow to each of the scanning computer systems in parallel;  
at each of the scanning computer systems, executing respective anti-virus scanning software having different, corresponding coverage of malicious code to scan the

flow for malicious code scanning and generating an alarm when the flow contains malicious code;

creating a signature of a piece of malicious code detected by at least one of the scanning computer systems detected in the flow when at least one of the scanning computers generates an alarm on the piece of malicious code;

causing signatures stored at the remote site detection system to be updated to include the signature of the piece of malicious code detected by said at least one of the scanning computer systems;

employing a countermeasure on the flow if at least one of the scanning computer generates an alarm on the piece of malicious code, including at least one of blocking the flow, quarantining the flow, and informing the recipient of the flow of the malicious code; and

detecting malicious code in incoming network traffic based on the signatures of malicious code stored thereat.

17. A front-end system, coupled to an external network and a plurality of scanning computer systems, said front-end system comprising one or more processors, a communications interface, and a computer-readable medium bearing instructions for causing the one or more processors upon execution thereof to perform the steps of:

receiving a flow of content from the external network, said flow including at least one of a hypertext markup file and a transferred file;

duplicating the flow to produce a plurality of copies of the flow; and

distributing the copies of the flow to each of the scanning computer systems in parallel.

18. A method for operating a front-end system, coupled to an external network and a plurality of scanning computer systems, said method comprising:

receiving a flow of content from the external network, said flow including at least one of a hypertext markup file and a transferred file;

5 duplicating the flow to produce a plurality of copies of the flow; and

distributing the copies of the flow to each of the scanning computer systems in parallel.

19. A computer-readable medium bearing instructions for operating a front-end system, coupled to an external network and a plurality of scanning computer systems, said instructions arranged, when executed, for causing one or more processors to perform the steps of:

receiving a flow of content from the external network, said flow including at least one of a hypertext markup file and a transferred file;

duplicating the flow to produce a plurality of copies of the flow; and

15 distributing the copies of the flow to each of the scanning computer systems in parallel.

20. A malicious code detection cluster, comprising:

an internal network coupled to a front-end processor and a detection management system;

20 a plurality of scanning computer systems coupled to the internal network and configured for:

receiving respective copies of a flow of content from the front-end processor in parallel, said flow including at least one of a hypertext markup file and a transferred file;

executing respective anti-virus scanning software having different, corresponding coverage of malicious code to scan the respective copies of the flow in parallel for malicious code; and  
transmitting an alarm to the detection management system when the flow contains  
5 malicious code as detected by at least one of the anti-virus scanning software.

21. A method of detecting malicious code in an internal network coupled to a front-end processor, a plurality of scanning computer systems, and a detection management system, said method comprising the steps of:

receiving respective copies of a flow of content from the front-end processor in  
10 parallel, said flow including at least one of a hypertext markup file and a transferred file;  
executing respective anti-virus scanning software having different, corresponding coverage of malicious code to scan the respective copies of the flow in parallel for  
malicious code; and  
15 transmitting an alarm to the detection management system when the flow contains malicious code as detected by at least one of the anti-virus scanning software.

22. A detection management system, coupled to a plurality of scanning computer systems, said detection management system comprising one or more processors, a communications interface, and a computer-readable medium bearing instructions  
20 arranged for causing the one or more processors upon execution thereof to perform the steps of:

receiving an alarm from one of the scanning computer systems when a flow of content scanned by the scanning computer systems in parallel contains malicious code, said flow including at least one of a hypertext markup file and a transferred  
25 file; and

employing a countermeasure on the flow if at least one of the scanning computers generates an alarm on a piece of the malicious code.

23. The detection management system according to claim 22, wherein the countermeasure includes at least one of blocking the flow, quarantining the flow, and  
5 informing the recipient of the flow of the malicious code.

24. The detection management system according to claim 22, wherein the detection management system is further coupled to a remote site detection system and said instructions are further arranged for causing the one or more processors to perform the steps of:

10 creating a signature of a piece of malicious code detected by at least one of the scanning computer systems in the flow when at least one of the scanning computers generates an alarm on the piece of malicious code; and  
causing signatures stored at the remote site detection system to be updated to include the signature of the piece of malicious code detected by said at least one of the  
15 scanning computer systems.

25. A method of managing malicious code detection, comprising:

receiving an alarm from one of the scanning computer systems when a flow of content scanned by the scanning computer systems in parallel contains malicious code, said flow including at least one of a hypertext markup file and a transferred  
20 file; and  
employing a countermeasure on the flow if at least one of the scanning computer generates an alarm on a piece of the malicious code.



26. The method according to claim 25, wherein said employing the countermeasure includes at least one of blocking the flow, quarantining the flow, and informing the recipient of the flow of the malicious code.

27. The method according to claim 25, further comprising:

5 creating a signature of a piece of malicious code detected by at least one of the scanning computer systems in the flow when at least one of the scanning computer generates an alarm on the piece of malicious code; and causing signatures stored at a remote site detection system to be updated to include the signature of the piece of malicious code detected by said at least one of the scanning computer systems.

10

28. A computer-readable medium bearing instructions for managing malicious code detection, said instructions arranged for causing the one or more processors upon execution thereof to perform the steps of:

15 receiving an alarm from one of the scanning computer systems when a flow of content scanned by the scanning computer systems in parallel contains malicious code, said flow including at least one of a hypertext markup file and a transferred file; and employing a countermeasure on the flow if at least one of the scanning computers generates an alarm on a piece of the malicious code.

20 29. The computer-readable medium according to claim 28, wherein the countermeasure includes at least one of blocking the flow, quarantining the flow, and informing the recipient of the flow of the malicious code.

creating a signature of a piece of malicious code detected by at least one of the

5

computers generates an alarm on the piece of malicious code; and

causing signatures stored at a remote site detection system to be updated to include

the signature of the piece of malicious code detected by said at least one of the

scanning computer/systems.

19/17

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280	281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305	306	307	308	309	310	311	312	313	314	315	316	317	318	319	320	321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340	341	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360	361	362	363	364	365	366	367	368	369	370	371	372	373	374	375	376	377	378	379	380	381	382	383	384	385	386	387	388	389	390	391	392	393	394	395	396	397	398	399	400	401	402	403	404	405	406	407	408	409	410	411	412	413	414	415	416	417	418	419	420	421	422	423	424	425	426	427	428	429	430	431	432	433	434	435	436	437	438	439	440	441	442	443	444	445	446	447	448	449	450	451	452	453	454	455	456	457	458	459	460	461	462	463	464	465	466	467	468	469	470	471	472	473	474	475	476	477	478	479	480	481	482	483	484	485	486	487	488	489	490	491	492	493	494	495	496	497	498	499	500	501	502	503	504	505	506	507	508	509	510	511	512	513	514	515	516	517	518	519	520	521	522	523</
--	---	---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-------